コンテンツセキュリティ　　2020 年 5 月 25 日

ブロックチェーン

執筆者: 安永憲司

世界中にちらばっている人たちで「しりとり」をするにはどうすればよいだろうか．もっとも簡単な方法は，参加者に $1, 2, \ldots, n$ と番号を割り振り，番号の小さい順に答えていく方法だろう．もう少しゲームとしておもしろくするため，回答は早い順でよく，回答の数がその人の得点というルールにしよう．せっかくなので，世界中の誰でも参加できるようにしよう．このゲームの一つの実現方法は，ウェブ掲示板を用意し，そこに書き込んでいく方法だろう．しかし，この方法では掲示板を管理する人が必要である．その人が管理をやめるとゲームができなくなる．それでは，管理者なしで実現する方法はないだろうか．これを実現するのがブロックチェーンである．

1　世界しりとりとその応用

管理者なしで掲示板を実現する一つの方法は，すべての参加者が同じ掲示板を手元に置いておくことだろう．全参加者の手元の掲示板が同じであれば，それをもとに次の回答を答えればよい．アリスが「あんごう」と言って始まり，次にボブが「うぉれっと」と答えた．この後に，チャーリーが「とらっぷどあ」，デーブが「とうちょうしゃ」とほぼ同時に答えたとすると，何が起きるだろうか．チャーリーから掲示板の更新を知ったエレンは，次に「あるごりずむ」と答え，デーブの掲示板を知ったフランクは「しゃーにごろ」と答えるかもしれない．つまり，しりとりの列が枝分かれしてしまい，ゲームにならなくなってしまう．

上記の問題は，回答をほぼ同時にすることができないような仕組みがあれば解決できる．誰かが回答して手元の掲示板を更新した後，それが全参加者に伝わるまでの間に別の回答が出てこなければ，全員が同じしりとりを続けることができる．

このアイディアにもとづいて電子的な「通貨」を実現したのが，ナカモトサトシによって提案されたビットコインである．そのデータ構造は，ブロックをチェーン状に繋いでいるため，基盤となる技術はブロックチェーンと呼ばれている．ブロックチェーンを使って，お金を実現する方法は，お金の出入りを記した「台帳」を管理することである．各個人に対するお金の付与，個人間のお金の受け渡し，これらの情報を時系列にすべて台帳に記載しておけばよい．お金を渡すことに対してその本人の電子署名があれば，それが不正行為でないといえる．ブロックチェーンは，それを時系列に並べた情報を，全参加者で共有する仕組みを与えている．特に，誰もが参加できるシステムとして実現しているのが特徴的である．

参加者を管理した上で，ブロックチェーン同様の機能を実現するプロトコルは，状態機械複製 (state machine replication) と呼ばれており，ビットコインの誕生以前から分散コンピューティング分野において研究されていた．ブロックチェーンと比較すると，参加者が管理できている分，高速な処理が可能だが，プロトコル自体は複雑であり，なかなか理解しづらい．また，参加者の不正についても，ブロックチェーンの方が高い耐性をもつ．

2　仕事の証明

しりとりゲームにおいて同時回答を防ぐ仕組みは，仕事の証明 (proof of work) と呼ばれるものである．ある種のパズルを解くことであり，そのパズルは，

1. 解が与えられるとその正しさを簡単に確認できる
2. 解を得るにはある程度の時間がかかる

という性質をもつ．パズルの解は，ある程度時間をかけなければ得られず，それは時間をかけたこと（仕事）の証明になるのである．

ビットコインでは，暗号学的なハッシュ関数を用いて，仕事の証明を比較的簡単に実現している．ハッシュ関数 $H : \{0,1\}^* \to \{0,1\}^n$ は，入力として前ブロックのハッシュ値 $h_{-1} \in \{0,1\}^n$, 当該ブロックの記載内容 m, および

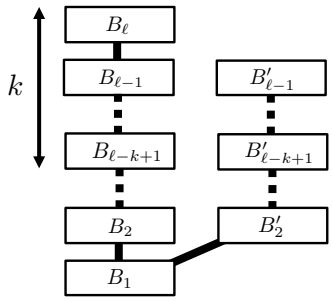

図 1　ナカモトプロトコルのブロックチェーン

ナンス $x \in \{0,1\}^n$ を受けとる．出力 $h = H(h_{-1}, m, x)$ がそのブロックのハッシュ値であるが，正しい解であるためには，h の先頭に 0 が一定数連続して登場する必要がある．つまり，関数の終域 $\{0,1\}^n$ を 0 から $2^n - 1$ までの整数値に対応させると，ある閾値 D に対し

$$H(h_{-1}, m, x) < D$$

を満たすナンス x を見つけるパズルである．ハッシュ関数であれば，(h_{-1}, m, x) が与えられたとき，その正しさを簡単に確認できる．また，理想的なハッシュ関数であれば，出力はランダムな値となるため，ナンスをひとつ選んだとき正しい解となる確率は $D/2^n$ 以下であり，正しい解を得るには $2^n/D$ 回程度ハッシュ関数を使う必要がある．別の言い方をすれば，正しい解を見つけた人は $2^n/D$ 回ハッシュ関数を計算したとみなせる．

この方法は，D の値を変えるだけでパズルの難しさを簡単に変えることができ便利である．実際に，ビットコインにおいても閾値 D をときどき見直すことで，仕事の証明にかかる時間を 10 分程度に保つようにしている．また，パズルの解を見つけた人にお金（ビットコイン）を与える仕組みを入れている．そのため，仕事の証明をすることは金の採掘に相当するため，採掘（マイニング）と呼ばれる．

3　ナカモトプロトコルの安全性

ナカモトサトシがビットコインの設計で提案したプロトコルの概要を説明する．ハッシュ関数 H に対し，初期ハッシュ値を $h_0 = H(0, \perp, 0)$ とする．ブロックチェーンは，ブロックの列（チェーン） $BC = (B_1, B_2, \dots)$ であり，各ブロックは $B = (h_{-1}, m, x, h)$ で構成される．正当なブロックであるためには，h_{-1} が直前のブロックのハッシュ値に一致し，$h = H(h_{-1}, m, x)$ であり，$h < D$ であればよい．チェーンに含まれるすべてのブロックが正当なとき，正当なチェーンと呼ぶ．

プロトコルとしては，各参加者は，その時刻における正当なチェーンが $BC = (B_1, B_2, \dots, B_\ell)$, 最後のブロックが $B_\ell = (h_{\ell-1}, m_\ell, x_\ell, h_\ell)$ のとき，記載内容 $m_{\ell+1}$ に対し，$h_{\ell+1} = H(h_\ell, m_{\ell+1}, x_{\ell+1}) < D$ を満たす $x_{\ell+1} \in \{0,1\}^n$ を探す．もし見つかれば，次の正当なブロック $B_{\ell+1} = (h_\ell, m_{\ell+1}, x_{\ell+1}, h_{\ell+1})$ を，すぐに参加者全員に伝える．これを繰り返すだけである．

正当なチェーンが $BC = (B_1, B_2, B_3, B_4, B_5)$ と $BC' = (B_1, B_2, B'_3, B'_4)$ のように複数あった場合，ブロック数の多い（長い）チェーンを採用することにする．こうすれば，枝分かれが起きたとしても，いずれはあるチェーンだけが最大の長さのものとして残り，それ以外は淘汰されることを期待するのである．また，同じ長さのチェーンが複数ある場合も，何らかのルールに従って採用するチェーンを選ぶ．

チェーンが $BC = (B_1, B_2, \dots, B_\ell)$ のとき，ブロック B_i のインデックス i をブロックの高さという．ブロックを下から積んでいった場合の高さに相当する．ブロックチェーンシステム全体では，複数のチェーンが存在する可能性があり，同じ高さに複数のブロックがあるかもしれない．また，ℓ をチェーンの長さと呼び，ブロック $B_{\ell-k+1}$ は深さ k のブロックと呼ぶ．

プロトコルの要件と攻撃モデル

ブロックチェーンへの攻撃者は，各参加者であるとし，一定割合の参加者が不正を行っても，問題が起きないことを保証したい．具体的には，プロトコルに求める性質として，実在性 (liveness) と一貫性 (consistency) を考える．実在性は，プロトコルに従えば，記載したい内容をチェーンに書き込むことができることを保証する．一貫性は，各参加者のチェーンには同じ内容が記載されていることを保証する．つまり，両方の性質を満たすとき，誰でもブロックチェーンに書き込むことができ，その内容は一意に定まる．プロトコルに従っている参加者を正直者，そうでない参加者を不正者と呼ぶ．正直者が採掘したブロックを正直ブロックと呼ぶことにする．このとき，要件を以下のように定める．

定義 1（実在性） ブロックチェーンプロトコルが実在性を満たすとは，以下のチェーン伸長 (chain growth) およびチェーン質 (chain quality) を満たすことである．

- チェーン伸長：十分大きな時刻 t において，正直者が採用するチェーンの長さは，確率 $1 - \mathsf{negl}(t)$ 以上で，$\Omega(t)$ である．
- チェーン質： 十分大きな時刻 t において，正直者が採用するチェーンにおける正直ブロックの割合は，確率 $1 - \mathsf{negl}(t)$ 以上で，$\Omega(1)$ である．

定義 2（一貫性） ブロックチェーンプロトコルが一貫性を満たすとは，ある時刻で正直者が採用したチェーンにおいて，ブロック B が高さ h，深さ k であるとき，それ以降の時刻で正直者が採用したチェーンの高さ h に，B 以外のブロックがある確率が $\mathsf{negl}(k)$ 以下のときである．

実在性は要件が二つに分かれているが，チェーン伸長により，時間に比例してチェーンが伸びることを保証し，チェーン質により，その一定割合が正直ブロックであることを保証している．記載したい内容があるとき，それをすべての参加者に伝え，正直者は受け取った内容をブロックに記載することにすれば，記載したい内容をチェーンに書き込むことができる．一貫性は，正直者同士のチェーンでは同じ高さに同じブロックがあることを保証している．注意したいのは，一貫性は，ブロックの深さ k に関して無視できる確率を除いて保証している点である．つまり，チェーンのある程度深いところまで進んだブロックでないと保証されない．

安全性の証明のため，以下の前提をおく．

(1) 正直者は，記載したい内容の有無に関わらず，常に採掘を行う．
(2) 採掘は無記憶であり，その成功確率は一定である．
(3) 通信遅延の上界がわかっている．

前提 (1) は，採掘によって金銭的利益があれば成り立つと考えられる．前提 (2) にある，採掘に成功する確率は，正直者全体で α，プロトコルを攻撃しようとする不正者全体で β とする．採掘が無記憶とは，過去の採掘の試みが，次の採掘の成功確率に影響しないことである．成功確率が一定のとき，採掘に成功する正直者・不正者の数は，それぞれパラメータ α, β のポワソン過程である．前提 (3) については，遅延がない場合を考えてもよいが，ナカモトプロトコルは，遅延上界 Δ が既知であれば正しく動作することを証明できる．実際のネットワークにおいても通信遅延は避けられず，また，遅延 Δ が安全性に影響することが理解できる．

確率の準備

確率過程とは，時刻 t をパラメータとしてもつ確率変数の族 $\{X_t\}$ であり，時間とともに変化する現象を捉えることができる．ポワソン過程は，時刻 t までにある事象が起きた回数を X_t とする確率過程であり，特に，各事象が独立に繰り返し起きる状況を捉えている．パラメータ λ のポワソン過程では，時刻 t_1 と時刻 t_2 の間の事象発生数は，他の期間に依存せず，パラメータ $\lambda(t_1 - t_2)$ のポワソン分布に従い，平均は $\lambda(t_1 - t_2)$ である．また，事象の発生する間隔は，同じパラメータ λ の指数分布に従う．事象が k 回発生するまでの期間を S_k とすると，それは独立同分

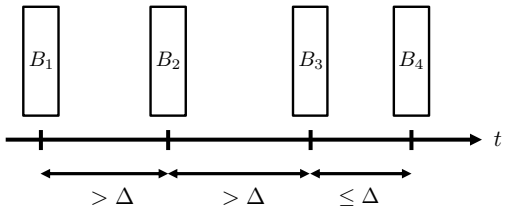

図 2 正直ブロックを採掘順に並べたもの．ブロック B_2 は前後十分であり，ブロック B_3 は前方十分である．

布な k 個の指数分布の和に等しく，アーラン分布である．以下では，裾確率に関する限界式を紹介する．

補題 3（チェルノフ限界） 独立な確率変数 $X_1, \ldots, X_n$ がそれぞれ $\{0,1\}$ の値をとるとき，$X = \sum_{i=1}^{n} X_i$ とし，X の期待値を μ とする．このとき，$0 < \delta < 1$ に対し，$\Pr[X > (1+\delta)\mu] < e^{-\Omega(\delta^2\mu)}$ かつ $\Pr[X < (1-\delta)\mu] < e^{-\Omega(\delta^2\mu)}$ である．

補題 4（ポワソンの裾） 確率変数 X がパラメータ μ のポワソン分布に従うとする．このとき，X の期待値は μ であり，$0 < \delta < 1$ に対し，$\Pr[X > (1+\delta)\mu] < e^{-\Omega(\delta^2\mu)}$ かつ $\Pr[X < (1-\delta)\mu] < e^{-\Omega(\delta^2\mu)}$ である．

補題 5（アーランの裾） パラメータ λ のポワソン過程において事象が k 回発生するまでの期間を表す確率変数を S_k とする．このとき，$0 < \delta < 1$ に対し，$\Pr\left[S_k > \frac{k}{(1-\delta)\lambda}\right] < e^{-\Omega(\delta^2 k)}$ かつ $\Pr\left[S_k < \frac{k}{(1+\delta)\lambda}\right] < e^{-\Omega(\delta^2 k)}$ である．

前後の十分な間隔

正直者が採掘に成功した時刻を順に並べたとき，その間隔が小さいと，通信遅延があるため，その採掘が無駄になってしまう可能性がある．つまり，通信遅延の影響がないような間隔で採掘されていれば，枝分かれせず，チェーンが伸びていく．

正直者が時刻 t にブロック B を採掘したとする．もし，時刻 $t-\Delta$ と t の間に他の正直者が採掘していないとき，B を前方十分と呼び，時刻 $t-\Delta$ と $t+\Delta$ の間にないとき，B を前後十分と呼ぶことにする（図 2 を参照）．不正者が採掘をしない間に，ブロックが前後十分となれば，チェーンは枝分かれなく伸びる．前方十分や前後十分は，正直ブロックに対する性質であることに注意しよう．

まず，次の補題が成り立つ．

補題 6 前方十分なブロックはそれぞれ異なる高さをもつ．また，前後十分なブロックはそれぞれが，その高さにある唯一の正直ブロックである．

証明: 前方十分なブロック B と B' が，この順に採掘されたとする．B は遅延上限の Δ 時間以内にすべての正直者に届いており，それは前方十分である B' を採掘する前である．すべての正直者は B を受け取った後，B の続きを採掘するため，B' は B と異なる高さをもつ．ブロックが前後十分であれば，後から採掘されたブロックとは高さが異なるため，その高さの唯一の正直ブロックである． □

ある期間におけるブロックの発生数を保証するため，損失パラメータ $\gamma = e^{-\alpha\Delta} < 1$ を導入する．これを使うことで，通信遅延を考慮した実質的な採掘確率を表すことになる．以降では，定数 $0 < \delta < 1$ を固定して使う．

補題 7 十分大きな期間 t の間に，確率 $1 - e^{-\Omega(\delta^2\gamma\alpha t)}$ 以上で，$(1-\delta/3)\gamma\alpha t$ 個以上の前方十分なブロックが採掘され，確率 $1 - e^{-\Omega(\delta^2\gamma^2\alpha t)}$ 以上で，$(1-\delta/3)\gamma^2\alpha t$ 個以上の前後十分なブロックが採掘される．

証明: まず，$\delta_1 \in (\delta/9, 2\delta/9)$ を選び，$n = (1-\delta_1)\alpha t$ が整数となるように十分大きな t をとる．期間 t の間の正直ブロックを採掘順に，ブロック $1, 2, \ldots, n+1$ と表し，その期間の直前の正直ブロックをブロック 0 と表す．事象 E_0 を，$S_n \leq t$ とする．つまり，期間 t で採掘が n 回以上発生する事象である．補題 5 より，$\Pr[\overline{E_0}] = \Pr[S_n > t] = \Pr\left[S_n > \frac{n}{(1-\delta_1)\alpha}\right] < e^{-\Omega(\delta_1^2 n)} = e^{-\Omega(\delta^2\alpha t)}$ である．

確率変数 X_i を，ブロック i が前方十分であるときに 1，それ以外は 0 をとるものとし，$X = \sum_{i=1}^{n} X_i$ とする．

同様に，Y_i は，ブロック i が前後十分であるときに 1，それ以外は 0 をとり，$Y = \sum_{i=1}^{n} Y_i$ とする．ポワソン過程の事象の発生間隔は，同じパラメータの指数分布に従うため，X_i が前方十分である確率は，パラメータ α の指数分布で Δ より大きな期間で事象が発生しない確率に等しく，$\Pr[X_i = 1] = e^{-\alpha\Delta} = \gamma$ である．事象 E_X を，$X \geq (1-\delta/3)\gamma\alpha t$ とする．また，$\delta_2 = \delta/3 - \delta_1 \in (\delta/9, 2\delta/9)$ とすると，$(1-\delta_2)(1-\delta_1) > 1-\delta/3$ である．チェルノフ限界より，$\Pr[\overline{E_X}] = \Pr[X < (1-\delta/3)\gamma\alpha t] \leq \Pr[X < (1-\delta_2)\gamma n] < e^{-\Omega(\delta_2^2\gamma n)} = e^{-\Omega(\delta^2\gamma n)}$ である．事象 $E_0 \cap E_X$ は，期間 t でブロックが n 個以上採掘され，そのうち $(1-\delta/3)\gamma\alpha t$ 個以上が前方十分のときである．上記より，$\Pr[\overline{E_0 \cap E_X}] < e^{-\Omega(\delta^2\gamma\alpha t)}$ であり，一つ目の主張が示された．

次に，E_Y を，$Y \geq (1-\delta/3)\gamma^2\alpha t$ とする．このとき，$Y_i = X_i X_{i+1}$ であるため $\Pr[Y_i = 1] = \gamma^2$ である．今回は，Y_i と Y_{i+1} が独立でないためチェルノフ限界は直接使えない．しかし，Y_i と Y_{i+2} は独立であるため，$Y = \sum_{\text{奇数 } i} Y_i + \sum_{\text{偶数 } i} Y_i$ と分解すればよい．二つの和それぞれにチェルノフ限界を適用すれば，$\Pr[\overline{E_Y}] = \Pr[Y < (1-\delta/3)\gamma^2\alpha t] < e^{-\Omega(\delta^2\gamma\alpha t)}$ となる．残りの証明は一つ目と同様に行えばよい． □

上記の補題をもとに，ナカモトプロトコルの安全性を示す．

実在性

定理 8 ナカモトプロトコルは，$\gamma\alpha > (1+\delta)\beta$ のとき実在性を満たす．特に，チェーン伸長については，確率 $1 - e^{-\Omega(\delta^2\gamma\alpha t)}$ 以上で長さが $(1-\delta/3)\gamma\alpha t$ 以上となる．チェーン質については，確率 $1 - e^{-\Omega(\delta^2\beta t)}$ 以上で正直ブロックの割合が $1 - (1+\delta)\frac{\beta}{\gamma\alpha}$ 以上となる．

証明: 最長チェーンの長さは，不正者による採掘で短くすることはできない．したがって，チェーン伸長は，補題 6 の一つ目と補題 7 の一つ目から導かれる．

チェーン質について，正直ブロックの割合が最小になる場合を考えよう．正直ブロックの数で最長のチェーンの下界が示されていることから，不正者も最長チェーンに対して採掘を行うことで，正直ブロックの割合を小さくすることができる．また，通信遅延があるため，正直ブロックが採掘されたとき，そのブロックよりも早く不正者のブロックを伝えて，正直ブロックの採掘を無駄にできるかもしれない．そのような攻撃がすべて成功したとき，正直ブロックの割合が最小になる．

ポワソンの裾より，時刻 t における不正ブロックの数 $N_1(t)$ は，確率 $1 - e^{-\Omega(\delta^2\beta t)}$ 以上で，$(1+\delta/3)\beta t$ 以下である．最長のチェーンの長さ $N_2(t)$ は，チェーン伸長より，確率 $1 - e^{-\Omega(\delta^2\gamma\alpha t)}$ 以上で，$(1-\delta/3)\gamma\alpha t$ 以上である．上記の考察より，最長チェーンの長さは $N_2(t)$ で，そのうち正直ブロックは $N_2(t) - N_1(t)$ 以上あるため，正直ブロックの割合は，

$$1 - \frac{N_1(t)}{N_2(t)} \geq 1 - \frac{(1+\delta/3)\beta t}{(1-\delta/3)\gamma\alpha t} > 1 - (1+\delta)\frac{\beta}{\gamma\alpha}$$

である．ここで，$(1+\delta/3)/(1-\delta/3) < 1+\delta$ を使っている． □

一貫性

定理 9 ナカモトプロトコルは，$\gamma^2\alpha > (1+\delta)\beta$ のとき一貫性を満たす．特に，ある時刻で正直者が採用したチェーンにおいてブロック B が深さ k のとき，それ以降の時刻で正直者が採用したチェーンにおいて B と同じ高さに B 以外のブロックがある確率は $e^{-\Omega(\delta^2 k)}$ 以下である．

証明: 一貫性が成り立たないと仮定すると，ある事象が起きることを示し，その後，その事象の生起確率は小さいことを示す．

正直者が採用したチェーンにおいてブロック B が深さ k であり，それ以降に正直者が採用したチェーンにおいて B と同じ高さに，別のブロック B^* があると仮定する．ここで，正直者が B^* のチェーンを採用し始めた時刻を t_1 とする．つまり，t_1 以前は，ブロック B を含むチェーンを採用し，t_1 以降は B^* の方の採用を始めた．時刻 t_1 における，この二つのチェーンの終端ブロックをそれぞれ B_1, B_1^* とする．また，B_0 を両チェーンの最後の共通正直

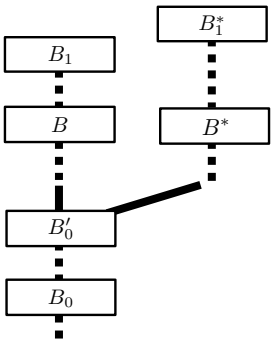

図 3 定理 9 の証明におけるブロックの配置．時刻 t_1 以降，ブロック B^* を含むチェーンを採用するようになり，その際の終端ブロックが B_1, B_1^*．

ブロック，B_0' を最後の共通ブロックとする．最後の共通ブロックが正直ブロックであれば B_0 と B_0' は同じである．ブロック B_1, B_1^*, B_0, B_0' の高さをそれぞれ h_1, h_1^*, h_0, h_0' とする．時刻 t_1 において，$h_1 \leq h_1^*$ である．ブロック B_0 の採掘時刻を t_0 とする．

時刻 t_0 と t_1 の間に不正者が採掘したブロック集合を A とする．時刻 $t_0 + \Delta$ と $t_1 - \Delta$ の間に採掘された前後十分なブロックの集合を S とする．

このとき，$|A| \geq |S|$ であることを示す．まず，任意のブロック $B_S \in S$ が前後十分のとき，その高さ h は $h_0 < h \leq h_1$ を満たすことを示す．正直者は，時刻 $t_0 + \Delta$ までにブロック B_0 を受けとる．そのため，時刻 $t_0 + \Delta$ 以降は h_0 より大きな高さしか採掘しない．したがって，$h > h_0$ である．また，B_S は前後十分であり，時刻 t_1 までに正直者に伝わる．正直者は時刻 t_1 まで B_1 を含むチェーンを採用しているため，$h \leq h_1$ である．

次に，各ブロック $B_S \in S$ に対し，それに対応する異なるブロック $B_A \in A$ が存在することを示すことで，$|A| \geq |S|$ を示す．ブロック $B_S \in S$ の高さを h とする．まず，$h \in (h_0, h_0']$ のとき，B_0 は最後の共通正直ブロックであるため，同じ高さ h にある不正者が採掘したブロック B_A をそれぞれ対応させることができる．次に，$h \in (h_0', h_1]$ のとき，同じ高さ h の枝分かれしたチェーンのブロックを対応させることができる．補題 6 の二つ目より，各 $B_S \in S$ は高さが異なるため，同じ高さに不正者が採掘したブロック B_A が必ず存在する．高さ h に関していずれの場合も，対応する B_A は，B_0 の続きとして採掘し，時刻 t_1 までに正直者に知られているため，$B_A \in A$ である．以上より，$|A| \geq |S|$ が示せた．

一方，$\gamma^2\alpha > (1+\delta)\beta$ のとき，$|A| \geq |S|$ となる確率は小さいことを示す．ここで，$t = t_1 - t_0$ とすると，A は期間 t の間に，S は期間 $t - 2\Delta$ の間に採掘されたブロックである．補題 7 の二つ目およびポワソンの裾より，$|S| > (1-\delta/3)\gamma^2\alpha(t-2\Delta)$ および $|A| < (1+\delta/7)\beta t$ となる確率は，いずれも $1 - e^{-\Omega(\delta^2\beta t)}$ 以上である．また，$t - 2\Delta > t/(1+\delta/7)$ を満たすように k を十分大きくとると，

$$|S| > \left(1 - \frac{\delta}{3}\right)\gamma^2\alpha(t-2\Delta) > \frac{1-\delta/3}{1+\delta/7}\gamma^2\alpha t > \frac{1-\delta/7}{1+\delta}\gamma^2\alpha t > \left(1+\frac{\delta}{7}\right)\beta t > |A|$$

が成り立つ．ここで，$\delta \in (0,1)$ に対し $\frac{1-\delta/3}{1+\delta/7} > \frac{1+\delta/7}{1+\delta}$ という関係と，仮定 $\gamma^2\alpha > (1+\delta)\beta$ を使っている．以上より，$|A| \geq |S|$ である確率は $e^{-\Omega(\delta^2\beta t)}$ 以下である．

最後に，確率 $e^{-\Omega(\delta^2\beta t)}$ を $e^{-\Omega(\delta^2 k)}$ で抑える必要がある．上記の証明において，期間 t の間に $2k$ 個以上のブロックが採掘されている．つまり，t はパラメータ $\lambda = \alpha + \beta$ のポワソン過程において事象が $2k$ 回発生するまでの間隔よりも大きい．したがって，アーランの裾より，確率 $1 - e^{-\Omega(\delta^2 k)}$ 以上で，$t > \frac{2k}{(1+\delta)(\alpha+\beta)}$ である．これより，$e^{-\Omega(\delta^2\beta t)} + e^{-\Omega(\delta^2 k)} \leq e^{-\Omega(\delta^2 k)}$ であり，定理が示された． □

実在性と一貫性の証明を行った．実在性の定理において，正直者の実質的な採掘確率は $\gamma\alpha$ であり，損失パラメータ $\gamma = e^{-\alpha\Delta}$ の分だけ損している．通信遅延 Δ が大きいと実質的な採掘確率が小さくなることがわかる．また，一貫性を満たすためには，不正者全体の採掘確率 β に対し，$\gamma^2\alpha > (1+\delta)\beta$ を満たす必要がある．もし遅延が小さく，$\Delta \ll 1/\alpha$ であれば，$\gamma \approx \gamma^2 \approx 1$ であり，$\alpha > (1+\delta)\beta$ を満たせばよい．つまり，正直者の採掘確率が不正者よりも少し勝っていればよいのである．